PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-219762
(43)Date of publication of application : 18.08.1995

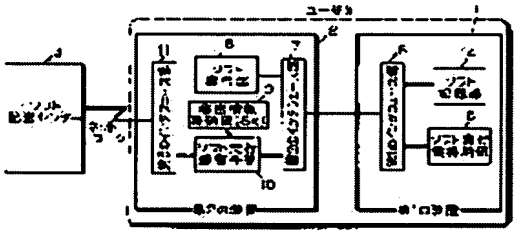
(51)Int.Cl. G06F 9/06
G06F 3/06
G06F 12/14
G09C 1/00

(21)Application number : 06-009228
(22)Date of filing : 31.01.1994

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MATSUZAKI NATSUME
MIYAJI MITSUKO

(54) SOFTWARE PROTECTION SYSTEM

(57)Abstract:
PURPOSE: To provide a method by which the copy of package software or software delivered from a network is prevented and execution in an arbitrary execution unit is easy.
CONSTITUTION: A system is provided with a first device storing software held by a user, a second device executing it and a software delivery center. The first device consists of a software recording part 4 storing ciphered software EA ciphered by a software key KA and a software execution key storage part 5 storing the software key KA. The so ware execution key storage part 5 is realized in an area where the copy of a chip and the like is difficult. In the case of package software, the first device including ciphered software EA and the software key KA is made into a package. In delivery by the network, the ciphered software key ciphered for the second device is decoded by using secret information peculiar to the second device and it is stored in the first device. At the time of executing software, the second device acquires the software key from the first device and software is decoded by using the key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－219762

(43)公開日　平成７年(1995)８月18日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ	9/06	５５０　Ｇ	9367－5B		
	3/06	３０４　Ｍ			
	12/14	３２０　Ｅ			
Ｇ０９Ｃ	1/00		9364－5L		

審査請求　未請求　請求項の数18　ＯＬ　（全 12 頁）

(21)出願番号　特願平6－9228

(22)出願日　平成６年(1994)１月31日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　宮地　充子
大阪府門真市大字門真1006番地　松下電器産業株式会社内

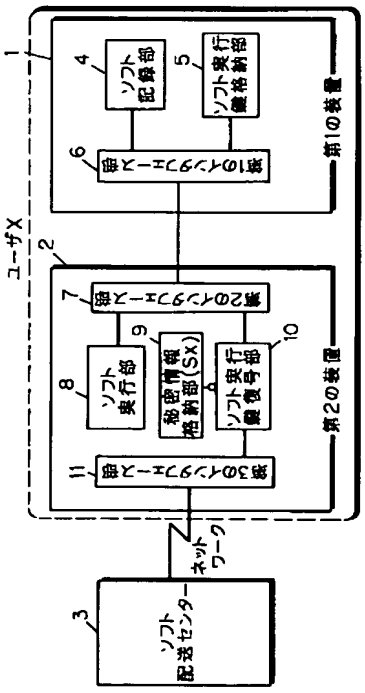
(74)代理人　弁理士　小鍛治　明　（外２名）

(54)【発明の名称】　ソフトウェア保護システム

(57)【要約】

【目的】　パッケージソフトまたはネットワークにより配送されたソフトのコピーを防止しつつ、任意の実行器での実行が容易な方法を提供する。

【構成】　システムは、ユーザが保持しソフトウェアを格納する第1の装置とこれを実行する第2の装置、およびソフト配送センターからなる。第1の装置は、ソフト鍵KAで暗号化された暗号化ソフトウェアEAを格納するソフト記録部4と、ソフト鍵KAを格納するソフト実行鍵格納部5を備える。ソフト実行鍵格納部5はチップなどのコピーが困難な領域に実現する。パッケージソフトの場合は、暗号化ソフトEAとソフト鍵KAを含んだ第1の装置をパッケージとする。ネットワークによる配送では、第2の装置用に暗号化された暗号化ソフト鍵を、第2の装置固有の秘密情報を用いて復号し、第1の装置に格納する。ソフト実行時には、第2の装置は第1の装置からソフト鍵を獲得し、これを用いてソフトの復号を行なう。



1

【 特許請求の範囲】

【 請求項1 】ソフトウェアを格納する第1 の装置と、所定の識別子を有し前記ソフトウェアを実行する第2 の装置と、ソフトを配送するソフト配送センターとを備え、ユーザは前記第1 の装置と前記第2 の装置を保持し、前記第2 の装置を用いて前記ソフト配送センターからソフトウェアを獲得したり、また前記第1 の装置を前記第2 の装置に装着してソフトウェアを実行するソフトウェア保護システムであって、

前記第1 の装置は、ソフトウェアを格納するソフト記録部と、そのソフトウェアを実行するために必要なソフト実行鍵を格納するソフト実行鍵格納部と、前記第2 の装置とデータのやり取りを行なう第1 のインタフェース部とを備え、

前記第2 の装置は、前記第1 の装置とデータのやり取りを行なう第2 のインタフェース部と、前記第1 の装置から得た前記ソフト実行鍵を用いて、前記第1 の装置の前記ソフト記録部に格納されているソフトウェアを実行する実行部と、前記第2 の装置の前記識別子に対応した固有の秘密情報を格納する秘密情報格納部と、前記ソフト配送センターとデータのやり取りを行なう第3 のインタフェース部と、前記第3 のインタフェース部を介して前記ソフト配送センターより獲得した暗号化ソフト実行鍵を、前記秘密情報を用いて復号して前記第2 、第1 のインタフェース部を介して、前記第1 の装置内の前記ソフト実行鍵格納部に格納するソフト実行鍵復号部とを備え、

前記ソフト配送センターは、前記第2 の装置とデータのやり取りを行ない、前記ソフト実行鍵を前記識別子を持つ第2 の装置用に暗号化し、得た暗号化ソフト実行鍵を前記第2 の装置に配送し、

前記第1 の装置におけるソフト実行鍵格納部と前記第2 の装置における秘密情報格納部は、ユーザが観察したり変更、複製できない領域に設定されているソフトウェア保護システム。

【 請求項2 】第1 の装置は、ケース内にソフト記録部を格納し、対応するソフトウェアのソフト実行鍵をチップに格納してそのケースに付加したことを特徴とする請求項1 記載のソフトウェア保護システム。

【 請求項3 】第1 の装置は、ソフトウェアを所定のソフト鍵で暗号化した暗号化ソフトウェアを格納するソフト記録部と、前記ソフト鍵を格納するソフト実行鍵格納部と、前記第2 の装置とデータのやり取りを行なう第1 のインタフェース部とを備え、

第2 の装置は、前記第1 の装置とデータのやり取りを行なう第2 のインタフェース部と、前記第1 の装置のソフト実行鍵格納部からソフト鍵を獲得して、これを用いて前記第1 の装置のソフト記録部に格納されている暗号化ソフトウェアを復号し実行する実行部と、第2 の装置の識別子に対応した固有の秘密情報を格納する秘密情報格

2

納部と、ソフト配送センターとデータのやり取りを行なう第3 のインタフェース部と、前記第3 のインタフェース部を介して前記ソフト配送センターより獲得した暗号化ソフト鍵を、前記秘密情報を用いて復号してソフト鍵を求め、前記第2 、第1 のインタフェース部を介して、第1 の装置の前記ソフト実行鍵格納部に格納するソフト実行鍵復号部を備えたことを特徴とする請求項1 記載のソフトウェア保護システム。

【 請求項4 】第1 の装置は、ソフトウェアを格納するソフト記録部と、前記ソフト配送センターが前記ソフトウェアに対してセンター秘密情報を用いて求めた署名情報を格納するソフト実行鍵格納部と、前記第2 の装置とデータのやり取りを行なう第1 のインタフェース部からなり、

第2 の装置は、前記第1 の装置とデータのやり取りを行なう第2 のインタフェース部と、前記ソフト実行鍵格納部から署名情報を獲得しこの正当性を確認し、正当である場合にのみ前記ソフト記録部のソフトウェアを実行する実行部と、第2 の装置の前記認証子に対応した固有の秘密情報を格納する秘密情報格納部と、前記ソフト配送センターとデータのやり取りを行なう第3 のインタフェース部と、第3 のインタフェース部を介して前記ソフト配送センターより獲得した暗号化された署名情報を、前記秘密情報を用いて復号して署名情報を求め、前記第2 、第1 のインタフェース部を介して前記第1 の装置の前記ソフト実行鍵格納部に格納するソフト実行鍵復号部とを備えたことを特徴とする請求項1 記載のソフトウェア保護システム。

【 請求項5 】第1 の装置にソフトウェア保護対策の有無を示すフラグ情報を格納すること、またはソフト実行鍵格納部の有無により、

前記第2 の装置の実行部が、第1 の装置のソフトウェア保護対策の有無を検出し、ソフトウェア保護対策がされていない第1 の装置の場合には、第1 の装置のソフト記録部のソフトウェアをそのまま実行することを特徴とする請求項1 記載のソフトウェア保護システム。

【 請求項6 】第1 の装置のソフト実行鍵格納部に、当該ソフトウェアの実行鍵および実行条件の情報を含め、ソフトウェア実行時に、第2 の装置の実行部がこれらの情報を第1 の装置から獲得し、その実行鍵が有効でありかつ実行条件を満たした場合にのみソフトウェアを実行することを特徴とする請求項1 記載のソフトウェア保護システム。

【 請求項7 】第2 の装置からの操作により、前記第1 の装置のソフト実行鍵格納部のソフト実行鍵および実行条件をマスク、およびマスクの解除ができることを特徴とする請求項6 記載のソフトウェア保護システム。

【 請求項8 】第2 の装置内のユーザが変更できない領域に、当該第2 の装置での実行条件を格納し、この実行条件を満たした場合にのみソフトウェアを実行することを

3

特徴とする請求項1 記載のソフトウェア保護システム。

【請求項9 】第2 の装置内のユーザが変更できない領域に、前記第2 の装置の実行部において実行したソフトウェアの履歴を保持することを特徴とする請求項1 記載のソフトウェア保護システム。

【請求項1 0 】第1 の装置のソフト実行鍵格納部に格納されているソフト実行鍵を特定の第2 の装置にバックアップする際に、

前記第1 の装置にバックアップの有無を示すフラグ情報を格納し、

バックアップ保管は、このフラグ情報がバックアップがないことを示している場合に前記第2 の装置からの操作により、第1 の装置のソフト実行鍵を第2 の装置に入力し、第2 の装置ではユーザが観察したり変更、複製できない領域にバックアップ保管し、前記第1 の装置のフラグ情報を更新し、

バックアップしたソフト実行鍵の使用は、第2 の装置は実行部において、前記第2 の装置に格納したソフト実行鍵を用いてソフトウェアを実行し、

また、前記第2 の装置からの操作により、このバックアップ保管したソフト実行鍵を第2 の装置から消去し、前記第1 の装置のフラグ情報を更新するよう構成したことを特徴とする請求項1 記載のソフトウェア保護システム。

【請求項1 1 】第2 の装置がある乱数を発生し、バックアップ保管時に第1 の装置から入力されたソフト実行鍵をこの乱数を用いて暗号化し、暗号化されたソフト実行鍵を別の記憶媒体に格納し、一方第2 の装置は前記発生した前記乱数を、ユーザが観察したり、変更、複製できない領域に格納し、

バックアップしたソフト実行鍵の使用は、第2 の装置が前記乱数を用いて前記別記憶媒体に格納されている暗号化ソフト実行鍵を復号し、ソフト実行鍵を獲得してソフトウェアを実行し、

また、前記第2 の装置での操作により、前記第2 の装置が、前記乱数を第2 の装置から消去し、前記第1 の装置のフラグ情報を更新することを特徴とする請求項1 0 記載のソフトウェア保護システム。

【請求項1 2 】ソフト配送センターが、特定の第2 の装置がソフト実行鍵を獲得していることを証明する証明書を、前記ソフト実行鍵と第2 の装置の識別子およびソフト配送センターの秘密情報を用いて求め、これを前記第2 の装置に発行し、前記第2 の装置がこの証明書を格納し、

前記第1 の装置にこの証明書の確認の要否を示すフラグ情報を格納し、このフラグ情報により証明書の確認が必要なソフトウェアの実行時には、実行をしている前記第2 の装置内の証明書の存在を確認し、さらに第2 の装置の識別子を獲得して証明書の正当性の確認を行ない、正当である場合にのみソフトウェアの実行を可能とすることにより、特定の第2 の装置でのみ当該のソフトウェアの実行を可能とする請求項1 記載のソフトウェア保護システム。

4

【請求項1 3 】特定の第2 の装置からの操作により、フラグ情報により証明書の確認が必要なソフトウェアの実行時であっても、有限回だけは前記第2 の装置での証明書の存在確認および正当性確認を行なわないように設定することにより、当該の第1 の装置を有限回だけ任意の第2 の装置で実行できるよう構成したことを特徴とする請求項1 2 記載のソフトウェア保護システム。

【請求項1 4 】第1 の装置内と第2 の装置の間で共通の第2 の秘密情報を用いた秘密鍵暗号通信が可能であり、ソフトウェアの実行開始時には、第2 の装置が乱数を発生しこれを保管し、その乱数を第1 の装置と共通の第2 の秘密情報で暗号化し、前記第1 の装置に送付し、前記第1 の装置が第2 の秘密情報でこれを復号して乱数を獲得し、獲得した乱数で前記ソフト実行鍵格納部内のソフト実行鍵を暗号化し、前記第2 の装置に送付し、前記第2 の装置ではこれを保管している前記乱数で復号して、ソフト実行鍵を求め、前記第2 の装置内の実行部に格納し、これを用いてソフトウェアを実行し、

ソフトウェア実行終了時には、第2 の装置の実行部に格納されているソフト実行鍵を消去することを特徴とする請求項1 記載のソフトウェア保護システム。

【請求項1 5 】第2 の装置とソフト配送センターとの間で、第2 の装置の前記秘密情報とこれに対応する公開情報およびソフト配送センターの保持するセンター秘密情報とこれに対応するセンター公開情報を用いた公開鍵暗号通信が可能であり、

前記第2 の装置が、ソフト配送センターから暗号化ソフト実行鍵を獲得する際に、前記第2 の装置が乱数を発生しこれを保管し、この乱数を前記センター公開鍵で暗号化した暗号化乱数と、この第2 の装置の認証子、獲得するソフト実行鍵の認証子および第2 の装置の前記秘密情報を用いて生成した申込証明書をソフト配送センターに送付し、

前記ソフト配送センターは、第2 の装置の認証子から第2 の装置の公開情報を求めてこれで前記申込証明書の正当性を確認し、前記センター秘密鍵を用いて暗号化乱数を復号して乱数を獲得した後、前記乱数と指定のソフト実行鍵を含んだ情報を第2 の装置の公開情報を用いて暗号化し、暗号化ソフト実行鍵として第2 の装置に送付し、

前記第2 の装置は送付された暗号化ソフト実行鍵を第2 の装置の前記秘密情報を用いて復号し、乱数とソフト実行鍵を獲得し、求めた乱数が前記発生し保管しているもとの乱数と一致している場合にのみ、求めたソフト実行鍵を有効とし、その後保管していた乱数を消去し、さらに、前記第1 の装置と前記第2 の装置は共通の第2 の秘密情報を保持し、

5

第2 の装置からの操作により、第1 の装置が乱数を発生しこれを保管し、その乱数を前記第2 の秘密情報で暗号化し、前記第2 の装置に送付し、前記第2 の装置が第2 の秘密情報でこれを復号して乱数を獲得し、前記ソフト配送センターから獲得したソフト実行鍵をこの乱数で暗号化し、前記第1 の装置に送付し、前記第1 の装置ではこれを前記保管している乱数で復号して、ソフト実行鍵を求め、前記第1 の装置内のソフト実行鍵格納部に格納し、その後第2 の装置内のソフト実行鍵を消去することを特徴とする請求項1 記載のソフトウェア保護システム。

【請求項１６】第2 の装置とソフト配送センターとの間で、公開鍵暗号通信の替わりに、共通の秘密情報を用いた秘密鍵暗号通信を用いた請求項１５記載のソフトウェア保護システム。

【請求項１７】ソフト配送センターが第2 の装置に配送するデータにソフト実行鍵の部数情報を含め、前記第2 の装置が前記ソフト配送センターから獲得した暗号化ソフト実行鍵を復号して、ソフト実行鍵を求め、前記ソフト配送センターが指定した部数分の第1 の装置内の前記ソフト実行鍵格納部に、このソフト実行鍵を格納することを特徴とする請求項1 記載のソフトウェア保護システム。

【請求項１８】第1 の装置にバックアップの有無を示すフラグ情報を格納し、
第2 の装置からの操作により、前記第1 の装置の実行鍵格納部に格納されているソフト実行鍵および前記第1 の装置のフラグ情報がバックアップが存在することを示している場合には第2 の装置内の実行鍵を消去し、この操作を行なったことを証明する情報を前記ソフト配送センターに送信することを特徴とする請求項1 記載のソフトウェア保護システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はデータ処理の分野に関し、特にマルチメディアソフトウェア保護機構に関する。さらに具体的には、本発明はCD-ROMなどで提供されるパッケージソフトや、ネットワークを介して提供されるソフトウェアの不正なコピーを防ぎつつ、任意の実行器でのソフトウェアの実行を可能とする。

【０００２】

【従来の技術】近年、種々のマルチメディア機器が開発され、ゲームや教育用のソフトを始めとする多くの有償マルチメディアソフトが販売されている。ところがそのソフトウェアの保護は不完全であり、不正コピーのソフトウェアが多く出回っているのが現状である。

【０００３】これを防ぐために特許法や著作権法等法律の規制があるが、同時にメカニズム面からのソフトウェア保護が必要である。

【０００４】例えばフロッピーディスク等の、ソフトウェアを格納する記録媒体のフォーマットを特殊なものにすることによって、OS(オペレーティング・システム) で提供されているコピー機能では複製ができないようにする方法がある。しかし、この方法でもビットごとにコピーを行なうタイプのコピーツールを用いれば多くの場合複製が可能である。また、正規のユーザにとっては、バックアップが作れないといった不都合も生じる。

【０００５】また、ソフトウェアを暗号化してコピー防止を行なう方法が提案されている。この方法は例えば特開平3 －０８３１３２号公報に示されている。図5 に構成を示す。

【０００６】図5 において１００はソフトウェアを供給する側、１０１はそれを実行する側の構成である。両者の間は例えばネットワークを介して接続されているとする。ソフトを供給する側においては、１０２は平文ソフトウェアをあるソフト鍵(特開平3 －０８３１３２号公報では、復号鍵と称している) で暗号化するソフト暗号部、１０３はユーザの識別子(ID) を入力としてある特定のユーザ固有の個別鍵を獲得する個別鍵獲得部、１０４は前記ソフト鍵を前記個別鍵を用いて暗号化する鍵暗号部である。また、ソフトを実行する側においては、１０５はその実行部固有の個別鍵を格納する個別鍵格納部、１０６は前記供給された暗号化ソフト鍵を、前記個別鍵を用いて復号しソフト鍵を取り出す鍵復号部、１０７は前記供給された暗号化ソフトウェアを、前記ソフト鍵を用いて復号しもとの平文ソフトウェアを求めるソフト復号部である。

【０００７】この構成において、まず、ソフト供給者１００はあるソフトウェアＡに対して1 つのソフト鍵KAを発生し、ソフト暗号部１０２でそのソフトウェアを暗号化し暗号化ソフトウェアEAを生成しておく。正規のユーザX は自身の識別子をソフト供給者に通知し、所定の手続きを行なう。これを受けたソフト供給者１００は、個別鍵獲得部１０３においてユーザX の個別鍵を獲得し、これを用いて鍵暗号部１０４で前記ソフト鍵を暗号化する。そしてユーザX にこの暗号化ソフト鍵EKAを前記暗号化ソフトウェアEAとともに送信する。ユーザX は送信されたEKA とEAを例えばフロッピーディスクやディジタルビデオディスク等の記録媒体に格納して任意の時に実行器１０１に装着して実行を行なう。ソフト実行時には、鍵復号部１０６は、個別鍵格納部１０５に格納されている個別鍵を用いて前記暗号化ソフト鍵EKA を復号しソフト鍵を求める。さらに、ソフト復号部１０７は同様に供給された暗号化ソフトウェアEAを、このソフト鍵を用いて復号し、もとの平文ソフトウェアＡを獲得する。

【０００８】第3 者はユーザX と同じ個別鍵を持っていないため、X のソフトウェア(暗号化ソフトウェアEAとユーザX 用に暗号化された暗号化ソフト鍵EKA) を保管している記録媒体を例えばコピーしても、これを第3 者の実行器では実行ができない。このことによりコピー防

7

止機能が実現されている。

【０００９】

【発明が解決しようとする課題】しかしながら、この従来のソフトウェア保護方式では正当なソフトウェアの持ち主であっても、ソフトウェアを自分の実行器以外では実行できない。

【００１０】ソフトウェアを他の場所で実行するためには、ソフトウェアを格納した記録媒体だけでなく、特定の実行部１０１までも移動させる必要がある。このことは、特定の実行部１０１がそのユーザに所属するものであり、また一般的には記録媒体に比べて大型で移動しにくいことを考慮すると、大きな問題点である。

【００１１】加えて、他のユーザにこのソフトウェアを譲ることも、例えばソフト配送センターによってソフト鍵を譲渡先のユーザ用に暗号化しなおしてもらう等の手続きが必要である。以上のことは現在のマルチメディアソフトの多くがゲームであり、ユーザが低年令層であるといった玩具的な側面からいって大きな問題点である。また、従来のコピー防止機能がないソフトウェアは、任意の実行器での実行やソフトウェアの譲渡、ソフトウェアの貸し借りがそのソフトウェアを格納したCD-ROMなどの記録媒体を移動するだけで可能である。これが、コピー防止機能を導入することによってできなくなるというのは、ユーザにとり不都合を生じるため、致命的な欠点といえる。

【００１２】さらに、この従来のソフトウェア保護方式はネットワークを介したソフト購入を前提としており、店頭でのソフト購入をそれほど考慮していない。想定できる店頭でのソフト購入形態としては例えば、店頭にてユーザXはソフト鍵を自分用に暗号化してもらい、暗号化したソフト鍵EKAをICカードのようにユーザに所属する媒体にその場で入れてもらう方法がある。そして実行時にはこのICカードを実行器に装着してソフトウェアの復号と実行を行なう。しかしこの形態は、自分の好みのソフトウェアを棚から自由に購入するといった従来から行なわれているソフト購入形態（以降パッケージソフト購入形態と称する）とはかけ離れており、市場に受け入れがたいものである。

【００１３】本発明は、上述の課題に鑑み、不法なコピーを防止しつつ、従来と同様にソフトウェアを任意の実行器で実行でき、さらにパッケージソフト購入形態とも整合するソフトウェア保護システムを提供することを目的としてなされたものである。また同時にソフトウェアの試用や返品といったサービス、および使っただけ支払うといった従量性課金を可能とするメカニズムも同様に提供する。

【００１４】

【課題を解決するための手段】ソフトウェアを格納する第1の装置と、所定の識別子を有し前記ソフトウェアを実行する第2の装置と、ソフトを配送するソフト配送セ

8

ンターとを備え、ユーザは前記第1の装置と前記第2の装置を保持し、前記第2の装置を用いて前記ソフト配送センターからソフトウェアを獲得したり、また前記第1の装置を前記第2の装置に装着してソフトウェアを実行するソフトウェア保護システムであって、前記第1の装置は、ソフトウェアを格納するソフト記録部と、そのソフトウェアを実行するために必要なソフト実行鍵を格納するソフト実行鍵格納部と、前記第2の装置とデータのやり取りを行なう第1のインタフェース部とを備え、前記第2の装置は、前記第1の装置とデータのやり取りを行なう第2のインタフェース部と、前記第1の装置から得た前記ソフト実行鍵を用いて、前記第1の装置の前記ソフト記録部に格納されているソフトウェアを実行する実行部と、前記第2の装置の前記識別子に対応した固有の秘密情報を格納する秘密情報格納部と、前記ソフト配送センターとデータのやり取りを行なう第3のインタフェース部と、前記第3のインタフェース部を介して前記ソフト配送センターより獲得した暗号化ソフト実行鍵を、前記秘密情報を用いて復号して前記第2、第1のインタフェース部を介して、前記第1の装置内の前記ソフト実行鍵格納部に格納するソフト実行鍵復号部とを備え、前記ソフト配送センターは、前記第2の装置とデータのやり取りを行ない、前記ソフト実行鍵を前記識別子を持つ第2の装置用に暗号化し、得た暗号化ソフト実行鍵を前記第2の装置に配送し、前記第1の装置におけるソフト実行鍵格納部と前記第2の装置における秘密情報格納部は、ユーザが観察したり変更、複製できない領域に設定された構成とする。

【００１５】

【作用】上記構成によれば、ソフト配送センターがソフトウェアを第1の装置のソフト記録部に格納し、前記ソフトウェアを実行するために必要なソフト実行鍵を、第3者が観察したり変更、複製できない領域のソフト実行鍵格納部に格納して第1の装置をパッケージソフトとして販売する。あるいは、ネットワークを介したソフト販売の際には、正規の手続きを行なったユーザ用にソフト実行鍵を暗号化し、これをユーザの第2の装置に送信する。ユーザ側では第2の装置の第3のインタフェース部を介してこの暗号化ソフト実行鍵を受信する。そして、自身の秘密情報を用いてこれを復号し、さらにこうして得たソフト実行鍵を前記第2、第1のインタフェースを介して第1の装置のソフト実行鍵格納部に格納する。以上のようにパッケージソフトまたは第2の装置を介してネットワークから得たソフトウェアを実行する際には、ユーザは第1の装置を任意の第2の装置に装着する。そして、第2の装置からの操作により、第2の装置は、第1の装置のソフト実行鍵格納部に格納されているソフト実行鍵を実行部にロードして、これを用いて第1の装置のソフト記録部に格納されているソフトウェアを実行する。

9

【００１６】

【実施例】図1は、本発明の一実施例の構成図である。なお、本実施例は請求項3の発明に係わるものである。

【００１７】本図において1は第1の装置、2は第2の装置であり、これら第1、第2の装置はユーザ側に所属するものである。ユーザは第2の装置に第1の装置を装着してソフトの実行を行なう。3はソフト配送センターであり、ソフトウェアをあるソフト鍵で暗号化し、パッケージソフトおよびネットワークを用いたソフト配送を行なう。ネットワークを用いたソフト配送のために、ユーザ側とソフト配送センター側はネットワークで接続されているものとする。

【００１８】第1の装置においては、4は暗号化ソフトウェアを格納するCD-ROMやディジタルビデオディスクといったソフトソフト記録部、5はその暗号化ソフトウェアを復号するためのソフト鍵を格納するソフト実行鍵格納部、6は第2の装置とソフト鍵などをやり取りする第1のインタフェース部である。ソフト実行鍵格納部5は複製や解析が困難である領域、例えばチップ内に実現する。

【００１９】また同図の第2の装置において、7は第1の装置とのソフト鍵などをやり取りする第2のインタフェース部である。8は第1の装置からソフト鍵と暗号化ソフトウェアを得て、復号、実行するソフト実行部である。9はこの第2の装置固有の秘密情報を格納する秘密情報格納部である。例えば特定のユーザXの保持する第2の装置（識別子をIDxとする）の秘密情報格納部9には、固有の秘密情報Sxが格納されている。１０はソフト配送センターから送られた暗号化されたソフト鍵を復号して第2、第1のインタフェース部を介して第1の装置のソフト実行鍵格納部5に格納するソフト実行鍵復号部である。１１はソフト配送センターとのやり取りを行なう第3のインタフェース部である。

【００２０】次に本実施例の動作を説明する。動作説明はソフト配送センターによるソフト配送時とユーザによるソフト実行時に分けて行なう。また、ソフトの配送は、パッケージソフトでの配送の場合と、ネットワークを介した配送の場合に分けて説明する。まず、パッケージソフトでの配送の場合について説明を行なう。

【００２１】ソフト配送センターは、あるソフトウェアAに対し1つのソフト鍵KAを生成する。そしてこのソフト鍵KAでソフトウェアAを暗号化し、第1の装置のソフト記録部に格納する。そして、ソフト鍵KAをチップ内のソフト実行鍵格納部に格納する。そしてこれらを例えば図2に示すようにケースに一体化して、パッケージソフトとして販売する。ケースに一体化したこのソフト保管形態は請求項2の発明に係わるものである。

【００２２】ソフト記録部は例えばCD-ROMやディジタルビデオディスクといった一般のものであるから、容易に複製を作成することができる。しかし、このソフトは暗

10

号化されており、復号して実行するにはソフト鍵が必要である。そしてソフト鍵は解析や複製が容易にできないチップ内に格納されているため、トータルとしてソフトウェアの複製は困難である。

【００２３】次に、ネットワークを介したソフト配送の場合について説明を行なう。ソフト配送センターが特定のユーザXにソフトを配送する場合について述べる。まず、ユーザXの第2の装置（識別子をIDxとする）には秘密情報Sxが格納されている。この秘密情報は各第2の装置ごとに異なっており、またユーザXですら観察したり取り出したりできないように例えばチップ内に格納されている。

【００２４】ソフト配送センターはパッケージソフト販売の場合と同様に、あるソフトウェアAに対し1つのソフト鍵KAを生成する。そしてこのソフト鍵を用いてソフトウェアを暗号化する。この暗号化ソフトウェアEAは例えばパブリックドメインにおいて、誰でもがこれを自分の第1の装置のソフト記録部にコピーできるようにしておく。また、ソフト配送センターが、ソフト購入手続きを行なったユーザに対してロードサービスを行なってもよいし、ユーザが自由に第3者からコピーしてもよい。なおネットワークを介したソフト購入の際には、ソフト記録部は読み書きが可能な媒体であるとする。

【００２５】次に、ソフト配送センターは、ソフトの購入手続きを行なったユーザXの第2の装置に対応してソフト鍵を暗号化し、暗号化ソフト鍵EKAをネットワークを介して第2の装置に配送する。ユーザXの第2の装置は、これを秘密情報格納部9に格納されているSxで復号し、もとのソフト鍵KAを獲得する。最後に、第2の装置は、装着された第1の装置のチップ内（ソフト実行鍵格納部）に、第2、第1のインタフェース部を介してこのソフト鍵を格納する。

【００２６】以上の手続きの結果、第1の装置は購入したパッケージソフトと同じ状態になる。

【００２７】以上のネットワークを介したソフト購入において、ソフト配送センターとユーザの第2の装置の間のやり取り、および第2と第1の装置の間のやり取りは例えば次のように乱数を用いて暗号化することにより、ソフト鍵の盗聴、なりすまし攻撃を防止する。なお、以下のプロトコルは請求項15の発明に係わるものである。

【００２８】まず、ソフト配送センターとユーザの第2の装置のやり取りの例を次に示す。図3にそのプロトコルを示している。同図において2はユーザX側の第2の装置、3はソフト配送センターである。ユーザXの第2の装置とソフト配送センターの間の通信には公開鍵暗号が使用されるとする。従って、第2の装置2にはソフト配送センターの公開鍵Pcとユーザの秘密鍵Sxが格納され、ソフト配送センター3にはソフト配送センターの秘密鍵Scと各ユーザの公開鍵が管理されているものとす

11

る。以下同図に従って、説明を行なう。
（１）ユーザ側の第2 の装置において、乱数raを発生しこれを保管する。
（２）第2 の装置において以下の情報を生成し、ソフト配送センターに送付する。
【００２９】(a) IDx: 第2 の装置の識別子
(b) IDA: ソフトウェアＡの識別子
(c) Epc(IDX || IDA || ra): IDX,IDA,ra を結合した情報をソフト配送センターの公開鍵を用いて暗号化する。なお、" || "の記号はデータを横に並べて結合することを示す。ここには公開鍵暗号を用いる。
【００３０】(d) Esx(M || Epc(IDX || IDA || ra)): 申込書Mと (c)の情報に対して、ユーザXの秘密鍵Sxを用いて署名を施す。ここでの署名は公開鍵暗号の署名機能を用いる。なおこれがソフトウェア申込証明書となる。
（３）ソフト配送センターは、(a) の情報をもとにユーザXの第2 の装置の公開鍵Pxを獲得し、これを用いて上記(d) のソフトウェア申込証明書の正当性を確認する。そしてソフト配送センターの秘密鍵Scを用いて (c)情報を復号し、IDx,IDA,raを得る。
（４）ソフト配送センターはソフトウェアＡのソフト鍵KAを、乱数raなどとともにユーザXの公開鍵Pxを用いて次のように暗号化してユーザXに送付する。
【００３１】(e) Epx(IDX || IDA || KA || ra): IDX,IDA,KA,raを結合した情報をユーザXの公開鍵を用いて暗号化する。ここには公開鍵暗号を用いる。
（５）ユーザXの第2 の装置では、送付された (e) の情報を内蔵されている秘密情報Sxを用いて復号し、得た乱数が（１）で保管している乱数raを同じ場合に、ソフト鍵KAを受け取る。その後、記憶している乱数raを消去する。
【００３２】以上のプロトコルにおいて、ネットワーク上に現われる (a) (b)の情報は公開情報であり、また、秘密情報を含む (c)～(e)の情報はすべて第2 の装置とソフト配送センターとの間で暗号化されてやり取りされる。また (c)～(e)の情報は乱数情報を含んでいるため毎回変化し、第3 者による盗聴やなりすましを防止している。
【００３３】上記プロトコルでは、（５）において第2 の装置はソフト鍵KAを受け取ったあとで、乱数raを消去している。このことによって、ユーザXの第2 の装置にはただ1 回だけしかソフト鍵のインストールができないようになっている。即ち、同じ (e) の情報を用いた2 回目以降のインストールでは、乱数raが失われているため、上記（５）のチェックでエラーを生じる。これはソフトウェアの返品を実現させるための機構であり、たとえ (e) の情報をコピーして保管しておいたとしても、ソフトウェアを返品したあとにソフト鍵の再インストールができない。従って、第1 の装置だけを返品するだけで第2 の端末にソフト鍵が残っていないことが保証できる。

12

【００３４】なお、ここでは第2 の装置とソフト配送センターの間で公開鍵暗号通信を仮定したが、これを秘密鍵暗号通信で行なってもよい。つまり、ソフト配送センターはすべての第2 の装置の識別子と対応する秘密情報を保持しており、秘密鍵暗号の共通鍵としてこれを用いる。これは請求項１６の発明に係わっている。
【００３５】次に、ソフト鍵をユーザの第2 の装置から第1 の装置に暗号送信するプロトコルの例を示す。図4にそのプロトコルを示している。同図に従って、以下説明を行なう。まず、すべての第1 の装置、第2 の装置には共通の秘密鍵S が格納されており、また秘密鍵暗号のアルゴリズムが格納されているとする。
（１）まず、第2 の装置からの操作により、第1 の装置は乱数rr1を発生し、保管する。
（２）第1 の装置は秘密情報Sで乱数rr1を暗号化し（Es(rr1)）、第2 の装置に送信する。ここでは秘密鍵暗号を用いる。
（３）第2 の装置はEs(rr1)を秘密情報Sで復号し、乱数rr1を得る。
（４）第2 の装置はソフト鍵KAを乱数rr1で暗号化し（Err1(KA)）、第2 の装置に送信する。その後ソフト鍵KA、乱数rr1を消去する。
（５）第1 の装置は第2 の装置から受け取ったErr1(KA)を乱数rr1を用いて復号し、KAを得て、チップ内のソフト実行鍵格納部に格納する。
【００３６】このプロトコルにおいて、第1 の装置と第2 の装置の間のデータは、秘密情報Sや乱数で暗号化されているため、第3 者はこれよりソフト鍵を求めることはできない。また乱数rr1を用いているため、毎回流れるデータが異なり、なりすまし攻撃を防いでいる。なお、（４）において第2 の装置からソフト鍵KAと乱数rr1を消去するのは、ソフト鍵が1 箇所だけに存在し、プロトコルの間でこれが複製されていないことを保証するためのものである。この機構により例えばソフトＡの返品の場合に、ユーザは装置1 だけを返品すればよく、ユーザ側の第2 の装置にソフト鍵のデータが残っていない。なお、もし第1 と第2 の装置の間の通信に誤りが生じた場合には第2 の装置に残っている暗号化ソフト鍵Err1(KA)を第1 の装置に再送するとよい。
【００３７】次に、ユーザによるソフト実行時の動作説明を行なう。ソフトウェアはパッケージソフトとして店頭で購入したものであろうと、ネットワークを介して購入したものであろうと例えば図2 に示す通り、暗号化ソフトウェアを格納したソフト記録部とそれを復号するためのソフト鍵を格納したチップという形態で保管される。そしてこのソフトウェアを実行する場合には、この第1 の装置を任意の第2 の装置に装着すればよい。
【００３８】すると、第1 の装置内のソフト実行鍵格納部に格納されているソフト鍵が第2 の装置のソフト実行部にロード（実質的には複写）される。そしてソフト実

行部内に暗号化ソフトが順次読み込まれ、ソフト鍵で復号されて実行される。

【００３９】この際のソフト鍵のロードのプロトコルの例は、図示は行なわないが前述した第2の装置から第1の装置へのソフト鍵の移動と同じく、共通の秘密鍵Sと乱数を用いる。なお、このプロトコルは請求項１４の発明に係わっている。

（１）第2の装置は乱数rr2を発生し、保管する。

（２）第2の装置は秘密情報Sで乱数rr2を暗号化し（ES(rr2)）、第1の装置に送信する。ここでは秘密鍵暗号を用いる。

（３）第1の装置はES(rr2)を秘密情報Sで復号し、乱数rr2を得る。

（４）第1の装置はソフト鍵KAを乱数rr2で暗号化し（Err2(KA)）、第2の装置に送信する。

（５）第2の装置は第2の装置から受け取ったErr2(KA)を乱数rr2を用いて復号し、KAを得て、実行部に格納する。

【００４０】また、ソフト実行終了時または第1の装置を離脱する際には、第2の装置に格納されているソフト鍵は消去する。この機構も、ソフト鍵が1箇所だけに存在し、プロトコルの間でこれが複製されていないことを保証するためのものである。例えばソフトの返品の場合にユーザは装置1だけを返品すればよい。

【００４１】以上述べたように本発明を用いれば、ソフト実行鍵が解析、複製が困難なチップに格納されていることにより、不正なコピーを防止している。かつ第1の装置は例えば図2に示すとおり携帯可能であり、第2の装置上で実行できる。また従来どおり、この第1の装置を渡すことにより、第3者へソフトを譲渡することができる。またネットワークを用いたソフト購入は個別情報を持つ第2の装置を介して行なう。そのためネットワークを介した課金にも対応できる。さらにある第2の装置を、ネットワークを介したソフト購入専用にすることも可能である。なお、その際にはソフト実行に用いる他の第2の装置は、必ずしもネットワークを接続する必要はない。以上述べたように本発明は第1、第2の装置の独立性が高い方法であるといえる。

【００４２】以上本発明を暗号化ソフトとそれを復号するソフト鍵で実現した一実施例に基づき説明したが、これが平文ソフトとそのソフトに対してのソフト配送センターの署名情報であってもよい。つまり、平文ソフトをソフト記録部に格納し、このソフト全体とソフト配送センターの秘密情報から算出される署名情報をソフト実行鍵として、観察したり複製できないチップに格納する。この実現方法は請求項4の発明に係わっている。

【００４３】そしてソフト実行時には、第2の装置では必ずそのソフトの署名情報の存在と正当性を確認し、確認できた場合にのみ実行するようにしておく。なおこの正当性確認の部分は第2の装置内のプログラムで実現さ

れ、このプログラムは変更ができない領域に格納されているとする。

【００４４】また、この署名情報を付加する方法を、先に述べたソフトウェアを暗号化する方法と同時に実現してもよい。署名情報を確認することによってソフト記録部に格納されているソフトが改変されていないこと（ソフトの完全性）を保証することにもなる。

【００４５】以上述べた実施例では、不正なコピーを防止しつつ任意の実行器での実行を可能としたソフトウェア保護システムの基本構成を実現している。この基本構成において、以下に述べる機能を実現することができる。

（１）ソフトウェア保護対策がされていないソフトの実行

この機能は請求項5の発明に係わっている。第1の装置のソフト記録部にソフトウェア保護対策がされているソフトかどうかのフラグを付加する。またはソフトウェア保護対策がされていないソフトの場合には、図2におけるソフト実行鍵を格納するチップを付加しない。第2の装置は、フラグやチップの有無により装着されている第1の装置のソフトが、保護対策がされているソフトかどうかを自動的に検出する。そしてソフトウェア保護対策がされているソフトの場合には第2の装置は、チップからソフト実行鍵を獲得して実行部において復号、実行を行なう。一方、ソフトウェア保護対策がされていないソフトの場合には第2の装置の実行部は、ソフト記録部よりソフトを読み込んでそのまま実行を行なう。

（２）第1の装置に実行鍵および実行条件、第2の装置にて実行制御

第1の装置に、例えばある定められた回数の実行だけが可能である回数券的なソフト実行鍵や、ある定められた期間内での実行が可能である定期券的なソフト実行鍵を備えることができる。なおこの部分は変更が困難であるチップ内に格納する。ソフトウェア実行時にソフト鍵をロードするのと同時に、これらの実行鍵をロードする。このロード時の改変や盗聴を防ぐため、この部分も勿論暗号化してロードする。そして第2の装置の実行部において、この条件を満たしているかを確認してからソフトウェアの実行を行なう。なお、この部分は請求項6の発明に係わっている。回数券的なソフト実行鍵の場合には第2の装置において実行した後、第1の装置のチップ内の情報を更新する必要がある。また定期券的なソフト実行鍵の場合には第2の装置の変更困難な部分に時刻情報を発生するクロック部が必要となる。

【００４６】さらに第1の装置は実行を許可する第2の装置の条件を設定することができる。例えばY組織に納入されている第2の装置にはある特定の識別子IDが格納されているとした場合、第1の装置にこのIDを持った第2の装置でのみ実行できるといった条件を設定できる。この設定がなされた第1の装置を第2の装置に装着する

15

と、第2 の装置の識別子を確認し、該当するIDの場合にのみ実行を行なう。

【００４７】また、ある第2 の装置からの操作により、上記のようなソフトの実行鍵や実行条件をマスクしたり、マスク解除することが実現できる。これは請求項7の発明に係わっている。例えばソフトの実行鍵として、上記回数券的なものと後述する第2 の装置に付加するクレジット的なものがあり、これらいずれを使用するかをユーザが選択できるとする。この場合、この機能を用いれば、あるユーザに第1 の装置を貸し出す場合に、回数券的な実行鍵をマスクして貸し出すことができる。するとソフトを借りたユーザは第1 の装置内の回数券的な実行鍵を使用することができず、自分の第2 の装置にクレジット情報として蓄えることになる。

（３）第2 の装置に実行鍵および実行条件、第2 の装置にて実行制御

これは請求項8 の発明に係わっている。例えば、第2 の装置にある上限値を設定し、この第2 の装置での実行はこの範囲内で行なう。これはあるソフトの実行回数であったり、種々のソフトのトータルの回数であってもよいし、支払金額の上限であってもよい。

（４）第2 の装置に実行履歴、試用

これは請求項9 の発明に係わっている。ある第2 の装置にて実行したソフトウェアの履歴を残しておき、この履歴に基づいて支払等を行なう。これにより、使用しただけ支払うといったクレジット的な「従量性課金」を実現することができる。実行履歴に基づいた支払はネットワークを介して手続きを行なってもよいし、例えばICカードのような携帯性のある媒体を介してオフラインで店頭にて支払を行なってもよい。

【００４８】試用プログラムの場合には、ある回数までは試用ということで無料で実行でき、ある回数以上になると課金を行なうといったことが、第2 の装置に実行履歴を残すことにより可能になる。

【００４９】なお、あるタイミングでの支払手続きを要求するために、前記（３）で述べたように例えば支払金額にある上限を設け、それ以上の実行は支払を済さないとできないようにすることも必要であろう。

（５）バックアップ

これは請求項１０の発明に係わっている。基本構成ではソフトウェアの実行鍵は第1 の装置に存在し、第2 の装置とは独立なものである。バックアップはこの実行鍵をある特定の第2 の装置に残すことにより実現する。なお、バックアップを2 箇所以上の第2 の装置に行なうことを防ぐために、バックアップの有無を示すフラグを設ける。

【００５０】まず、バックアップ保管時には第1 の装置を第2 の装置に装着し、第2 の装置からの操作により行なう。第2 の装置は第1 の装置がまだバックアップされていないことをフラグで確認して、第1 の装置からソフト実行鍵が読み込む。そしてこれを第2 の装置のユーザが観測、変更、複製できない領域に保管する。そして第１の装置のバックアップフラグを更新する（バックアップありを示す）。

16

【００５１】例えば第1 の装置のソフト実行鍵格納のチップが壊れた場合には、上記バックアップを行なった第２の装置において、保管されているソフト実行鍵を用いて、暗号化ソフトウェアの復号、実行を行なう。

【００５２】また、第2 の装置からの操作により第2 の装置内のバックアップ保管された実行鍵を消去できるようにする。この場合、第1 の装置のバックアップフラグを更新する（バックアップなしを示す）。

【００５３】なお、バックアップするソフト実行鍵が多くて別の記録媒体を使用する場合には、まず第2 の装置が乱数を発生しこの乱数を第2 の装置内のユーザが観測、変更、複製できない領域に保管する。そして第1 の装置から得たソフト実行鍵をこの乱数を用いて暗号化し、別記録媒体に記録する。バックアップ実行時にはこの別記録媒体を装着し、第2 の装置に格納した乱数を用い暗号化されたソフト実行鍵を復号し、そのあとソフト実行鍵を用いて暗号化ソフトウェアの復号、実行を行なう。そして、バックアップを引き上げる際には、前記第２の装置内の乱数を消去し、前記第1 の装置のバックアップフラグを更新する。この部分は請求項1 1 の発明に係わっている。

（６）特定の第2 の装置でのみ動作するソフトウェア

これは請求項1 2 、１３の発明に係わっている。ある特別なソフトウェアは、ソフト配送センターの許可を受けた第2 の装置でのみ動作するように設定できる。このためのメカニズムを以下に示す。ソフト配送センターは、動作を許可する第2 の装置に対し、証明書を発行する。証明書はソフトウェア自身、ユーザの第2 の装置の識別子およびソフト配送センターの秘密情報を用いたディジタル署名である。この発行は、店頭、またはネットワークを介してその第2 の装置に対して行なわれる。

【００５４】そして、フラグ情報などにより証明書の確認が必要と設定されたある特別なソフトウェアの実行の際には、実行している第2 の装置の識別子とソフト配送センターの公開情報を用いてこの証明書を確認する。そして、それが正しい場合にのみ実行を行なう。この証明書はその識別子を持つ許可された第2 の装置でのみ有効であるため、当該のソフトウェアは特定の第2 の装置でないと動作しない。

【００５５】ところが、こういったソフトウェアであっても、仮に他の第2 の装置で実行したい場合がある。このため有限回数だけ任意の第2 の装置での実行を許可する設定が、特定の第2 の装置においてできるようにしておく。この設定は第1 の装置になされ、設定がされていると有限回数だけはそのソフトウェアは証明書を確認せずに任意の第2 の装置で動作する。

17

（７）ソフトの返品

以上述べてきたように、本発明ではソフト実行鍵をプロトコルの間で複製しない機構を備えている。これを利用して、有効なソフト実行鍵を格納した第1の装置だけをソフト配送センターに返却することにより、ソフトの返品が成立する。つまり、ユーザ側の第2の装置等にソフト実行鍵が残留していないことが保証できる。

【００５６】また、第2の装置からの操作で第1の装置およびバックアップがある場合にはその第2の装置内のソフト実行鍵を消去する。そしてこの操作を行なったことを証明する情報を生成し、その第2の装置からソフト配送センターに送付することによりオンラインでのソフトウェアの返品が実現できる。これは請求項１８の発明に係わっている。

（８）複数ソフト実行鍵の配送

これは、請求項１７の発明に係わっている。ネットワークを介したソフト配付において、ソフト配送センターが第2の装置に配送するデータにソフト実行鍵の部数情報を含める。前記第2の装置は、暗号化ソフト実行鍵を復号して、ソフト実行鍵を求める。そして、ソフト配送センターが指定した部数情報に基づき、その部数分の第1の装置にソフト実行鍵を格納する。このことによりソフト配送センターから第2の装置への1回の配送で、複数の第1の装置にソフト実行鍵を格納することができる。

【００５７】

【発明の効果】以上の説明から明らかなように、請求項１、３、４の発明においてはパッケージソフトとしての第1の装置はソフトウェアとその実行鍵を保持し、その実行鍵はユーザが観察したり変更、複製できない領域に保管されている。一方、ネットワークを介したソフト実行鍵の獲得は次の手順で行ない、結果的にはパッケージソフトと同じ第1の装置を得ることができる。まず固有の秘密情報を内蔵している第2の装置が、ソフト配送センターから暗号通信を用いてソフト実行鍵を得る。次に第2の装置は固有の秘密情報を用いて、復号したソフト実行鍵を装着されている任意の第1の装置に乱数を用いた暗号通信で送信する。ソフト配送センターと第2の装置、第1の装置の間はそれぞれ暗号通信であるため、ここからソフト鍵が求めることは困難である。以上のことより本発明方式は、パッケージソフト販売の場合でも、ネットワークを介したソフト販売の場合でも、ソフトの保管および実行形態は同じであり、両者に整合した方法であるといえる。また、本発明では第1の装置と第2の装置の独立性が高いため、第1の装置は任意の第2の装

18

置で実行可能である。またネットワークを介したソフト獲得は任意の第2の装置から行なうことができる。そしてソフト実行鍵はユーザが観察したり変更したり複製できない例えばチップに格納されており、トータルとして第1の装置の複製を防止している。

【００５８】この第1の装置を実現するためには、請求項2に示す通り、従来のソフト記録媒体にソフト実行鍵を格納するためのチップを付加することが必要となる。しかしチップ自身は大量生産によりコストを下げることができ、従来に比べてのコストアップはわずかである。

【００５９】また、この基本構成に多少のメカニズムを導入することにより、次のことが可能となる。

・ソフトウェア保護対策のないソフトウェアの実行

・回数券的実行鍵、定期券式実行鍵や種々の実行条件の設定

・ソフトウェアの試用、返品サービス

・第2の装置に実行履歴を残し、これに基づいた従量性課金

・特定の第2の装置にソフト実行鍵をバックアップ

・特定のソフトはある特定の第2の装置でのみ動作

【図面の簡単な説明】

【図1】本発明に係わるソフトウェア保護システムの一実施例の構成図

【図2】上記一実施例の第1の装置の一実現形態を示す図

【図3】上記一実施例の第2の装置とソフト配送センター間の暗号通信の一実現方式を示す図

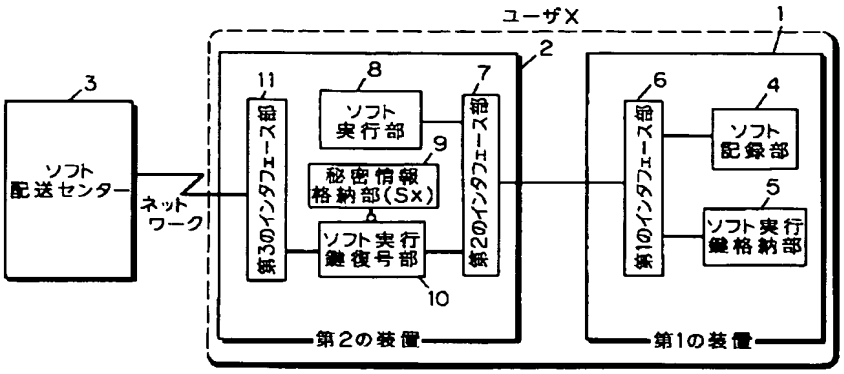
【図4】上記一実現例の第1の装置と第2の装置間の暗号通信の一実現方式を示す図

【図5】従来技術に係わるソフトウェア保護システムの構成図

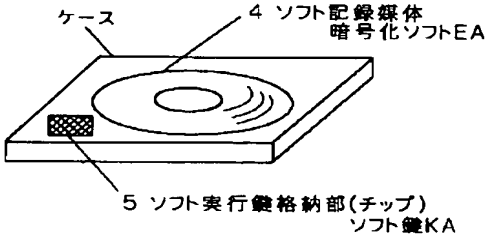
【符号の説明】

1　第1の装置
2　第2の装置
3　ソフト配送センター
4　ソフト記録部
5　ソフト実行鍵格納部
6　第1のインタフェース部
7　第2のインタフェース部
8　ソフト実行部
9　秘密情報格納部
１０　ソフト実行鍵復号部
１１　第3のインタフェース部

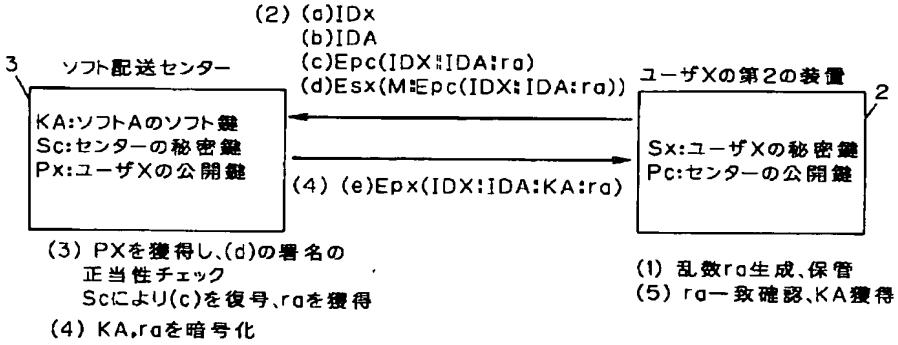
【 図1 】


ユーザX
1
2
3
11
8
7
6
4
ソフト配送センター
ネットワーク
第3のインタフェース部
ソフト実行部
秘密情報格納部(Sx)
ソフト実行鍵復号部
第2のインタフェース部
第1のインタフェース部
ソフト記録部
ソフト実行鍵格納部
5
9
10
第2の装置
第1の装置

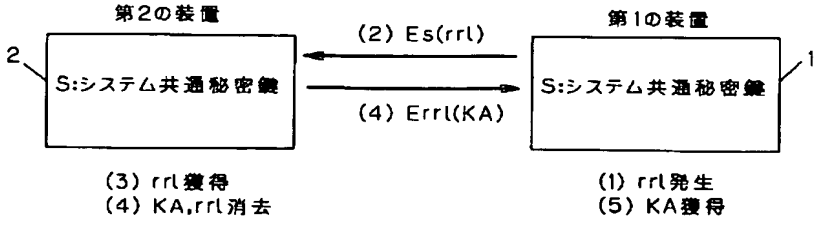
【 図2 】


ケース
4 ソフト記録媒体
暗号化ソフトEA
5 ソフト実行鍵格納部(チップ)
ソフト鍵KA

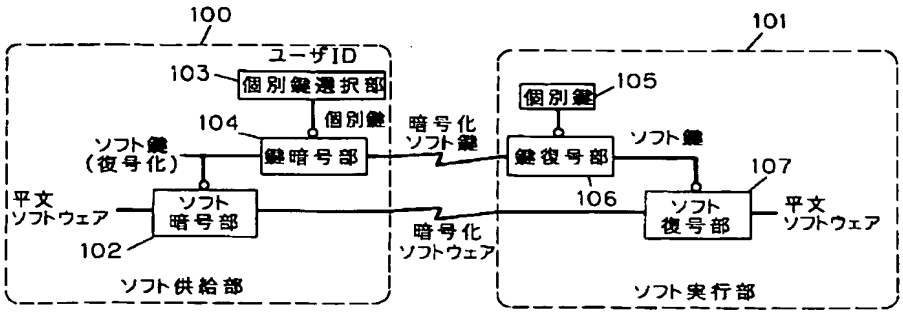
【 図3 】


(2) (a)IDx
(b)IDA
(c)Epc(IDX:IDA:ra)
(d)Esx(M:Epc(IDX:IDA:ra))
3
ソフト配送センター
ユーザXの第2の装置
2
KA:ソフトAのソフト鍵
Sc:センターの秘密鍵
Px:ユーザXの公開鍵
Sx:ユーザXの秘密鍵
Pc:センターの公開鍵
(4) (e)Epx(IDX:IDA:KA:ra)
(3) PXを獲得し、(d)の署名の
正当性チェック
Scにより(c)を復号、raを獲得
(4) KA,raを暗号化
(1) 乱数ra生成、保管
(5) ra一致確認、KA獲得

【 図4 】


第2の装置
第1の装置
(2) Es(rrl)
2
1
S:システム共通秘密鍵
S:システム共通秘密鍵
(4) Errl(KA)
(3) rrl獲得
(4) KA,rrl消去
(1) rrl発生
(5) KA獲得

【 図5 】


100
101
ユーザID
103
個別鍵選択部
個別鍵
104
ソフト鍵
(復号化)
鍵暗号部
暗号化
ソフト鍵
個別鍵
105
鍵復号部
ソフト鍵
107
106
平文
ソフトウェア
ソフト
暗号部
102
暗号化
ソフトウェア
ソフト
復号部
平文
ソフトウェア
ソフト供給部
ソフト実行部